SPARQ SECURITY POLICY

July 20, 2011

1. Grantee and sub-grantee administrators can only be approved by the SCSEP national office. The official grantee contact person may request that the Department of Labor (DOL) authorize up to three (3) grantee administrator accounts per grantee and one (1) sub-grantee administrator account per sub-grantee. Grantee administrators will serve as back-ups for the sub-grantee administrator. Administrators must be employees or contractors working under the direct supervision of the grantee or sub-grantee. Participant staff may not be administrators.

2. Each request for a grantee or sub-grantee administrator user account must be sent by e-mail to Phil Hostetter (Hostetter.Phil@dol.gov) and Dana Graham (Graham.Dana@dol.gov) at DOL, with a copy to BCT (help@scsep-help.com). The request must be accompanied by scanned copies of the Security Rules for SPARQ Administrators (Attachment A) containing the signatures of each proposed administrator. (Alternately, the signed attachments may be faxed to 202-693-3817 – attn: Dana Graham.)

The request must state that copies of the Security Rules for SPARQ Administrators (Attachment A) containing the signatures of each proposed administrator have been submitted to DOL. The request must also state that each proposed administrator has signed the Security Rules for SPARQ Users (Attachment B), which does not need to be sent to DOL. These forms may be downloaded from the BCT Web site.

The official grantee contact person is required to keep copies of the signed forms on file for three (3) years after the individual ceases to be a grantee or sub-grantee administrator.

3. DOL will reply to the e-mail with a copy to BCT (help@scsep-help.com) indicating its approval, denial, or request for additional information. Upon DOL's approval of the request, BCT will establish the administrator account(s) in SPARQ.

4. Administrators may designate as SPARQ users only those individuals who are employees or contractors working under the direct supervision of the grantee or of an entity that has a legally binding sub-grantee relationship with the grantee. Participant staff may be designated as SPARQ users. Researchers, IT vendors, potential sub-grantees, and other parties that have no formal legal responsibility for administering the SCSEP program may not be given direct access to SPARQ.

5. When registering new users, the grantee or sub-grantee administrator will identify the capacity of the user on the SPARQ registration screen. A drop-down menu will offer choices for employee, participant staff, contractor, and other. (If other is chosen, a 50-character text box will appear and must be filled in with an explanation of the user's capacity.) The administrator will also certify at the time of submitting the registration that the new user has signed a copy of the Security Rules for SPARQ (Attachment B). This form may be downloaded from the BCT Web site. The administrator is required to keep copies of the signed form on file for three (3) years after the individual ceases to be a registered user.

6. When a new user first logs on to SPARQ, the user will be required to certify that he or she will comply with all of the security requirements contained in Attachment B.

7. SPARQ administrators and users may not share their passwords with anyone, even other administrators or users.

8. Each SPARQ user must have one, and only one, account and User ID. The person using an account must provide his or her own personal information for the following SPARQ fields: First Name, Last Name and E-mail Address. The User ID must include at least the first six characters of the last name of that person (or full name if less than six characters). Each SPARQ user must have his or her own unique e-mail address.

9. The SPARQ audit system tracks various user transactions by User ID. The SPARQ User Accounts page indicates which accounts have not been used for 90 days by displaying an account status of "Expired." Grantee administrators must monitor the status of the accounts under their control at least every quarter. Administrators will have 30 days after the account is noted as expired to either reset the passwords of expired accounts where the user is still active with SCSEP and still requires current access to SPARQ or request that these accounts be deleted, whichever is appropriate. Any user account that has been expired for more than 30 days (that is, has not been used for 120 days) will be deleted.

10. When an administrator ceases to have the necessary relationship with SCSEP to justify access to SPARQ, the official grantee contact person must immediately notify DOL and request that administrator status be removed for that individual. When a SPARQ user ceases to have the necessary relationship with SCSEP to justify access to SPARQ, the relevant administrator must immediately deregister that user.

ATTACHMENT A

Security Rules for SPARQ Administrators

All SPARQ administrators must abide by the following rules as a condition of their access to SPARQ and their status as administrators:

- Administrators must sign and at all times abide by the Security Rules for SPARQ Users.
- Administrators may create user accounts only for employees; contractors working under the direct supervision of the grantee/sub-grantee or of an entity that has a legally binding sub-grantee relationship with the grantee/sub-grantee; and participant staff.
- Administrators will verify the identity of any person who requests to have a password reset.
- Administrators will be diligent in educating users about the need to abide by the Security Rules and in monitoring their use of SPARQ.
- Administrators will immediately delete the role(s) of any user who no longer has a SCSEP capacity that permits SPARQ access and will notify BCT to delete the user's account.

Certification by Administrator:

I hereby certify that I have received a copy of the Security Rules for SPARQ Administrators and understand that my access to SPARQ is conditional upon my compliance with these rules.

_____
Name

_____
Date

ATTACHMENT B

Security Rules for SPARQ Users

The Department of Labor provides the SCSEP Performance and Results QPR (SPARQ) system to you subject to the following Security Rules. This policy may be updated periodically without notice. Any updates to the policy shall be effective immediately when posted. The most current version of this policy is available by clicking the Security Rules link on the SPARQ home page. This system is provided and operated by the United States Government. Following are the rules of behavior that users must adhere to when using SPARQ:

Unauthorized access or use of the system for any purpose other than official government business is punishable by a fine, imprisonment, or both. Your use of the system may be monitored (18 U.S. Code 1030).

You are entirely responsible for any and all activities that occur under your system account on the Web site.

Unauthorized attempts to upload information or change information on this Web site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996.

Only authorized users are allowed access to SPARQ data.

Data (printed or non-printed) must not be divulged to any individual who is not specifically authorized to receive such information.

Sharing user login information – i.e., your username and password – is strictly prohibited. You must take the necessary steps to ensure that others do not use your account to gain unauthorized access to this system.

Data must not be tampered with, changed, deleted, or altered unless the user is authorized to do so.

Data must not be disclosed without proper authorization from the management of the Office of Workforce Investment.

SPARQ may not be used to collect personal information (e.g., for mass mailing) or to conduct personal business without the consent of the U.S. Department of Labor. You are not allowed to use SPARQ to send commercial messages (e.g., advertisements) or unsolicited bulk emails (e.g., informational announcements such as loss of family notices).

Posting material or information that is unlawful or inappropriate, such as obscene materials, inappropriate content, or inappropriate language, on this site is prohibited. Users will be held solely responsible for any information posted and published to this Web site that is in violation of this policy. Users shall be held responsible for ensuring that any information or content posted/published is in fact appropriate for the intended recipient(s).

Any fraudulent activities, including illegally using someone else's account, posting system messages, or e-mailing customers for personal gain or concerns, is prohibited.

SPARQ may not be used to breach the security of any system user or to gain access to another person's (internal or external) computer, software, or data.

SPARQ may not be used in any attempt to circumvent the system authentication or security of any account, network, or host. Please note that this would include, but is not limited to, accessing data that is not intended for your information, logging into a server or account to which you are not authorized to gain access, or probing the security of other networks.

Using tools to compromise system security of SPARQ, such as password-guessing programs, cracking or packet sniffing tools, or any network probing tools, is strictly prohibited, and legal action may be taken against you if you use such tools.

Any attempt to disrupt or deny operation of SPARQ is strictly prohibited.

Transmitting viruses, via e-mail or otherwise, when using this system is not allowed.

It is prohibited to sell any of the data or information gained from SPARQ.

Users shall be responsible for notifying DOL's Office of Workforce Investment immediately of any unauthorized use of their account or any other breach of security in regards to these polices. DOL will investigate any and all suspected violations of these policies and reserves the right to take corrective or legal action against the violator. If an investigation is warranted, a user's account access may be disabled. As a system user, you are responsible for ensuring that your use of the system complies with the stated policies. **Any system user who does not agree to be bound by these polices should immediately discontinue use of this system and should notify DOL's Office of Workforce Investment.**

The rules outlined here must be followed by all system users of SPARQ. Any abuse of these policies may be punishable by law. Questions regarding complaints, violations, or the requirements of this policy may be directed to Phil Hostetter (Hostetter.Phil@dol.gov) for appropriate handling and resolution.

The Department of Labor, Employment and Training Administration, Office of Information Systems and Technology's Security Officer is responsible for supporting and enforcing the established policies set forth in these Security Rules. The policies set forth in the Security Rules have been put in place to protect SPARQ users from the adverse impact that can result from intentional violations of the rules. If you believe you have been the victim of activities that are in violation of the rules, the Office of Information Systems and Technology will take appropriate action to investigate and attempt to resolve the alleged violation. You may report your concern or incident to this division at the DOL Security and Emergency Management Office (SecurityOffice.DOL@dol.gov). Please make sure you include the date and time of the incident, log files (if appropriate), examples or any other information that may be useful to the investigation and verification of the incident, as well as your name and phone number or e-mail address so this office can contact you directly.

DOL reserves the right to disable your account access without notice for violation of these polices.

Certification by User:

I hereby certify that I have received a copy of the Security Rules for SPARQ Users and understand that my access to SPARQ is conditional upon my compliance with these rules.

_____ _____

Name Date